



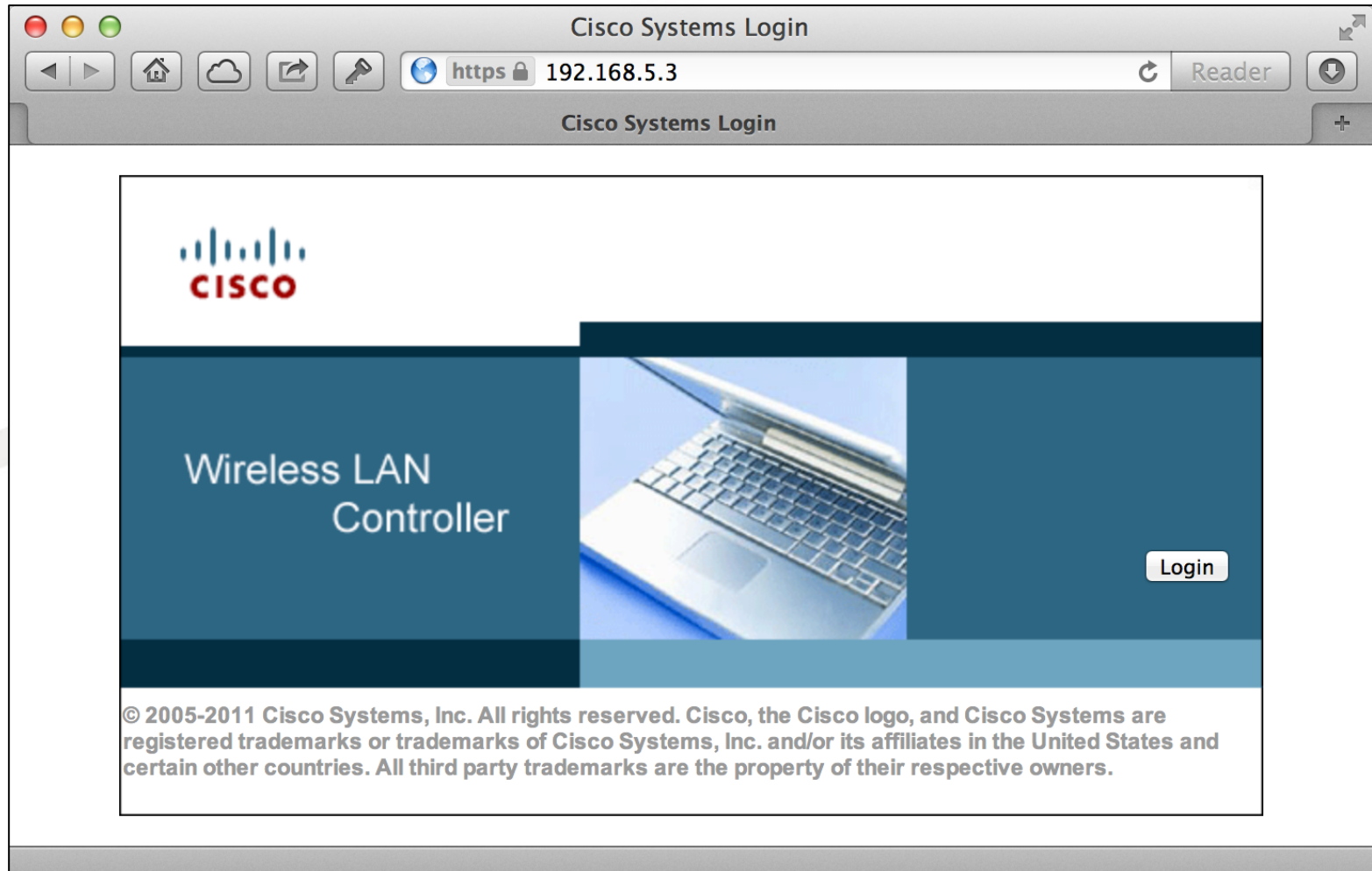
IDENTITY MANAGER INTEGRATION WITH CISCO WLC

SECTION B

WHAT YOU WILL LEARN

- > Configure an SSID for Web Authentication
- > Add IDM as the RADIUS Server
- > Set IDM as the external web portal
- > Configure IDM for Cisco Wireless LAN Controllers

LOGIN TO THE WEB CONSOLE



ADD IDM AS A RADIUS AUTH SERVER

WLC5508

https://192.168.5.3/screens/frameset.html

WLC5508

Save Configuration

CISCO

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMM

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Fallback
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
- Local EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth
- TrustSec SXP
- Advanced

RADIUS Authentication Servers > New

Server Index (Priority) 1

Server IP Address 192.168.1.27

Shared Secret Format ASCII

Shared Secret

Confirm Shared Secret

Key Wrap ☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number 1812

Server Status Enabled

Support for RFC 3576 Enabled

Server Timeout 2 seconds

Network User ☒ Enable

Management ☒ Enable

IPSec ☐ Enable

1. Specify the IDMs IP address

2. Specify a shared secret (same as used on IDM)

ADD IDM AS A RADIUS ACCT SERVER

WLC5508

https://192.168.5.3/screens/frameset.html

WLC5508

Save Config

CISCO

MONITOR WLANs CONTROLLER WIRELESS **SECURITY** MANAGEMENT

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting**
 - Fallback
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
- Local EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth
- TrustSec SXP
- Advanced

RADIUS Accounting Servers > New

| | |
|-------------------------|--|
| Server Index (Priority) | 1 |
| Server IP Address | 192.168.1.27 |
| Shared Secret Format | ASCII |
| Shared Secret | |
| Confirm Shared Secret | |
| Port Number | 1813 |
| Server Status | Enabled |
| Server Timeout | 2 seconds |
| Network User | <input checked="" type="checkbox"/> Enable |
| IPSec | <input type="checkbox"/> Enable |

1. Specify the IDMs IP address

2. Specify a shared secret (same as used on IDM)

CREATE A PRE-AUTHENTICATION ACL

WLC5508

https://192.168.5.3/screens/frameset.html

WLC5508

Save Configuration | Ping | Logout | Refresh

CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELI

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Fallback
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
 - Local EAP
 - Priority Order
 - Certificate
- Access Control Lists**
 - Access Control Lists
 - CPU Access Control Lists
 - FlexConnect ACLs

Access Control Lists > New

Access Control List Name preauth

ACL Type ☒ IPv4 ☐ IPv6

1. Give it a name

2. Select IPv4

ADD A DESTINATION RULE

WLC5508

https 192.168.5.3/screens/frameset.html

WLC5508

Save Configuration | Ping | Logout | Refresh

CISCO

MONITOR | WLANs | CONTROLLER | WIRELESS | HELP | FEEDBACK

Security

AAA

- General
- RADIUS
 - Authentication
 - Accounting
 - Fallback
- TACACS+
- LDAP
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies
- Password Policies

Local EAP

Priority Order

Certificate

Access Control Lists

- Access Control Lists
- CPU Access Control Lists
- FlexConnect ACLs

Wireless Protection Policies

Web Auth

TrustSec SXP

Advanced

Access Control Lists > Rules > New

< Back | Apply

Sequence: 1

Source: Any

Destination: IP Address: 192.168.1.27, Netmask: 255.255.255.255

Protocol: TCP

Source Port: Any

Destination Port: HTTPS

DSCP: Any

Direction: Any

Action: Permit

1. Sequence 1

2. Destination set to IDM

3. Protocol TCP

4. Destination Port HTTPS

5. Action Permit

ADD A SOURCE RULE

The screenshot shows the Cisco WLC5508 configuration interface. The browser address bar displays `https://192.168.5.3/screens/frameset.html`. The page title is `WLC5508`. The navigation bar includes `MONITOR`, `WLANS`, `CONTROLLER`, `WIRELESS`, `HELP`, and `FEEDBACK`. The `WIRELESS` tab is selected. The left sidebar shows the `Security` menu with options like `AAA`, `RADIUS`, `TACACS+`, `LDAP`, `Local Net Users`, `MAC Filtering`, `Disabled Clients`, `User Login Policies`, `AP Policies`, `Password Policies`, `Local EAP`, `Priority Order`, `Certificate`, `Access Control Lists`, `Wireless Protection Policies`, `Web Auth`, `TrustSec SXP`, and `Advanced`. The main content area is titled `Access Control Lists > Rules > New`. It contains a form for creating a new rule. The fields are: `Sequence` (value: 2), `Source` (value: IP Address), `Destination` (value: Any), `Protocol` (value: TCP), `Source Port` (value: HTTPS), `Destination Port` (value: Any), `DSCP` (value: Any), `Direction` (value: Any), and `Action` (value: Permit). Five red callout boxes with numbers 1 through 5 point to the following fields: 1. Sequence 2, 2. Source set to IDM, 3. Protocol TCP, 4. Source Port HTTPS, and 5. Action Permit. The `Source` field is also expanded to show `IP Address` (value: 192.168.1.27) and `Netmask` (value: 255.255.255.255). The `Apply` button is visible in the top right corner.

1. Sequence 2

2. Source set to IDM

3. Protocol TCP

4. Source Port HTTPS

5. Action Permit

ADD A NEW SSID

The screenshot shows the Cisco WLC5508 configuration interface. The browser address bar displays `https://192.168.5.3/screens/frameset.html`. The page title is "WLC5508". The navigation bar includes links for [MONITOR](#), [WLANs](#) (selected), [CONTROLLER](#), [WIRELESS](#), [SECURITY](#), [MANAGEMENT](#), [COMMANDS](#), [HELP](#), and [FEEDBACK](#). The main content area is titled "WLANs > New". It contains the following fields:

- Type:
- Profile Name:
- SSID:
- ID:

Three red callout boxes with white text provide instructions:

1. Set type to WLAN (for wireless)
2. Give the profile a name
3. Set the SSID

SET LAYER 2 TO BE AN OPEN NETWORK

The screenshot shows the Cisco WLC5508 configuration interface in a web browser. The browser address bar shows the URL `https://192.168.5.3/screens/frameset.html`. The page title is "WLC5508". The navigation bar includes links for "MONITOR", "WLANS", "CONTROLLER", "WIRELESS", "SECURITY", "MANAGEMENT", "COMMANDS", "HELP", and "FEEDBACK". The "WLANS" tab is selected, and the "Edit 'Wireless Hotspot'" page is displayed. The "General" tab is active, and the "Layer 2" sub-tab is selected. The "Layer 2 Security" dropdown menu is set to "None". A red callout box with the text "1. Set to None" points to the "None" option in the dropdown menu. The "MAC Filtering" checkbox is unchecked. The "Fast Transition" checkbox is also unchecked.

WLC5508

Save Configuration | Ping | Logout | Refresh

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANS

WLANS > Edit 'Wireless Hotspot'

< Back Apply

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security 6 None

MAC Filtering 9 ☐

Fast Transition

Fast Transition ☐

SET LAYER 3 TO USE IDM

WLC5508

https 192.168.5.3/screens/frameset.html

WLC5508

Save Configuration | Ping | Logout | Refresh

MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs

WLANs > Edit 'Wireless Hotspot'

< Back Apply

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 3 Security None

☒ Web Policy 1

☒ Authentication

☐ Passthrough

☐ Conditional Web Redirect

☐ Splash Page Web Redirect

☐ On MAC Filter failure10

Preauthentication ACL IPv4 preauth IPv6 None

Over-ride Global Config ☒ Enable

Web Auth type External(Re-direct to external server)

URL https://192.168.1.27/portal/192.168.5.3

1. Set to None
2. Set to Web Policy
3. Specify pre-auth acl
5. Over-ride Global Config
6. Set External Web Auth
7. Set URL as per next slide

CRU NETWORKS®

IDM URLs

- > The URLs that the controller needs to redirect the user to are on IDM.
- > The initial redirection should go to `https://[IDM-Name-or-IP]/portal/[Controller-IP]`
 - The IDM-Name-or-IP should match the SSL certificate common name on IDM
 - The Controller-IP is the IP address of the controller
 - Don't enter the [] brackets

SET AAA SERVERS

The screenshot shows the Cisco WLC5508 configuration interface for the 'Wireless Hotspot' WLAN. The 'AAA Servers' tab is selected under the 'Layer 3' section. The configuration includes sections for Radius Servers, Authentication Servers, Accounting Servers, Radius Server Accounting, Local EAP Authentication, and Authentication priority order for web-auth user.

1. Set to IDM

2. Set to IDM

Foot Notes

- 1 Web Policy cannot be used in combination with IPsec
- 2 FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
- 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 4 Client MFP is not active unless WPA2 is configured
- 5 Learn Client IP is configurable only when FlexConnect Local Switching is enabled
- 6 WMM and open or AES security should be enabled to support higher 11n rates
- 7 Band Select is configurable only when Radio Policy is set to 'All'
- 8 Value zero implies there is no restriction on maximum clients allowed.
- 9 MAC Filtering is not supported with FlexConnect Local authentication
- 10 MAC Filtering should be enabled.
- 11 Guest tunneling, Local switching, DHCP Required should be disabled.
- 12 Max-associated-clients feature is not supported with FlexConnect Local Authentication.
- 13 Fast Transition is supported with WPA2 and open security policy

SET AAA SERVERS

WLC5508

https://192.168.5.3/screens/frameset.html

WLC5508

Save Configuration | Ping | Logout | Refresh

CISCO

MONITOR | **WLANs** | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK

WLANs

WLANs > Edit 'Wireless Hotspot'

< Back | Apply

General | Security | QoS | **Advanced**

Allow AAA Override ☒ Enabled

Coverage Hole Detection ☒ Enabled

Enable Session Timeout ☒ 1800
Session Timeout (secs)

Aironet IE ☒ Enabled

Diagnostic Channel ☐ Enabled

Override Interface ACL IPv4: None IPv6: None

P2P Blocking Action: Disabled

Client Exclusion ☒ Enabled 60
Timeout Value (secs)

Maximum Allowed Clients: 0

Static IP Tunneling ☐ Enabled

Wi-Fi Direct Clients Policy: Disabled

Maximum Allowed Clients Per AP Radio: 200

Off Channel Scanning Defer

Scan Defer Priority: 0 1 2 3 4 5 6 7

Foot Notes

1 Web Policy cannot be used in combination with IPsec
2 FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
4 Client MFP is not active unless WPA2 is configured
5 Learn Client IP is configurable only when FlexConnect Local Switching is enabled
6 WMM and open or AES security should be enabled to support higher 11n rates
7 Band Select is configurable only when Radio Policy is set to 'All'.
8 Value zero implies there is no restriction on maximum clients allowed.
9 MAC Filtering is not supported with FlexConnect Local authentication
10 MAC Filtering should be enabled.
11 Guest tunneling, Local switching, DHCP Required should be disabled.
12 Max-associated-clients feature is not supported with FlexConnect Local Authentication.
13 Fast Transition is supported with WPA2 and open security policy

DHCP

DHCP Addr. Assignm

Management Frame Protection (MFP)

MFP Client Protection 4: Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255): 1

802.11b/g/n (1 - 255): 1

NAC

NAC State: None

Load Balancing and Band Select

Client Load Balancing: ☐

Client Band Select 2: ☐

Passive Client

Passive Client: ☐

1. Set to AAA Override

SET WLAN TO ENABLED

The screenshot shows the Cisco WLC5508 configuration interface. The browser address bar displays `https://192.168.5.3/screens/frameset.html`. The page title is "WLC5508". The navigation bar includes links for "MONITOR", "WLANs", "CONTROLLER", "WIRELESS", "SECURITY", "MANAGEMENT", "COMMANDS", "HELP", and "FEEDBACK". The "WLANs" section is active, showing a list of WLANs on the left. The main content area is titled "WLANs > Edit 'Wireless Hotspot'". It features tabs for "General", "Security", "QoS", and "Advanced". The "General" tab is selected, showing the following configuration:

| | |
|------------------------------|--|
| Profile Name | Wireless Hotspot |
| Type | WLAN |
| SSID | wireless-hotspot |
| Status | <input checked="" type="checkbox"/> Enabled |
| Security Policies | Web-Auth (Modifications done under security tab will appear after applying the changes.) |
| Radio Policy | All |
| Interface/Interface Group(G) | management |
| Multicast Vlan Feature | <input type="checkbox"/> Enabled |
| Broadcast SSID | <input checked="" type="checkbox"/> Enabled |

A red callout box with the text "1. Set status to Enabled" points to the "Enabled" checkbox under the "Status" field.

ADD THE CONTROLLER TO IDM

1. Enter a name (used for description only)

2. Enter the IP address of the controller

3. Enter the same shared secret used on the controller RADIUS setup

4. Specify Cisco WLC for the Type

Client Attributes SNMP MAC

Name: Cisco WLC

Device IP Address / Prefix Length: 192.168.5.3
For example 192.168.1.1/32 or fec0:0001/128

Secret:

Type: Cisco WLC
If your RADIUS client vendor is not listed please s

Description:

Change-of-Authorization

COA: ☐

Port: 3799

Save Cancel



Thank you